

# De phish wordt duur betaald

Koops, E.J.; Wiemans, F.P.E.

*Published in:*
Nederlands Juristenblad

*Publication date:*
2005

B.J. Koops & P. Wiemans (2005), 'De phish wordt duur betaald', *Nederlands Juristenblad* 80 (14), p. 741.

# De phish wordt duur betaald

Een van de grootste groeimarkten in de misdaad is het fenomeen 'phishing': het slinks hengelen naar bankgegevens, wachtwoorden en pincodes. Via bijvoorbeeld nepsites, valse netpostberichten of leuke sms'jes worden achteloze burgers uitgenodigd om hun financiële gegevens op te sturen, die dan echter niet bij Postbank.nl of Wehkamp terechtkomen, maar bij oplichters en – steeds meer georganiseerde – misdaadbendes.[1] Het aantal phishing-websites groeide in de tweede helft van 2004 elke maand met 24%,[2] een indicatie van de explosieve stijging van dit fenomeen.
Wie het strafrecht erop naslaat om te zien wat er tegen phishing te doen valt, vindt wel enkele mogelijkheden.[3] De meest voor de hand liggende bepaling, oplichting, is echter lang niet altijd van toepassing. De phish wordt daarom duur betaald door slachtoffers. Oplichting (art. 326 Sr) stelt slechts strafbaar degene die op listige wijze 'iemand beweegt tot de afgifte van enig goed, tot het ter beschikking stellen van gegevens met geldswaarde in het handelsverkeer, tot het aangaan van een schuld of tot het teniet doen van een inschuld'. Bij het aftroggelen van pincodes en wachtwoorden is geen sprake van een schuld of inschuld. Evenmin wordt 'enig goed' afgegeven, want gegevens zijn nu eenmaal geen 'goed' in strafrechtelijke zin.[4] En er worden ook geen 'gegevens met geldswaarde in het handelsverkeer' afgestaan, want de wetgever doelt hiermee op gegevens die op de legale markt verhandelbaar zijn – zoals adressenbestanden of programmatuur.[5] Pincodes, kredietkaartnummers en dergelijke zijn niet legaal verhandelbaar – ze hebben alleen een eventuele geldswaarde op de zwarte markt. Het op slinkse wijze ontfutselen van een pincode is daarom geen oplichting.
Opmerkelijk genoeg is het onder geweld dwingen van iemand om zijn pincode te noemen inmiddels wél strafbaar als afpersing. Hoewel het object van art. 317 Sr vergelijkbaar was met art. 326 (enig goed, gegevens met geldswaarde in het handelsverkeer, schuld of inschuld), heeft de wetgever in 2003 de bepaling aangepast, juist om het afpersen van pincodes strafbaar te stellen. Hiertoe is de zinsnede 'met geldswaarde in het

[1] Zie voor een goed overzicht van uitvoeringsvormen en mogelijke tegenmaatregelen Gunter Ollman, *The Phishing Guide. Understanding & Preventing Phishing Attacks*, September 2004, <http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf>. Meer informatie is te vinden bij de Anti-Phishing Working Group, <http://www.antiphishing.org/>. Dat cybercriminaliteit steeds vaker het werk is van georganiseerde misdaad wordt ook bevestigd door een recente verkenning van de Europese computercriminaliteit door de Zwitserse beveiligingsexpert Peter Troxler, aldus 'Computerinbraak steeds vaker werk bende', *de Volkskrant* 11 februari 2005.
[2] *Phishing Activity Trends Report*, December 2004, beschikbaar op <http://antiphishing.org/>.
[3] Afhankelijk van hoe er precies 'gephisht' wordt, kan men zich schuldig maken aan hacken (art. 138a Sr), gegevensmanipulatie (art. 350a Sr), diefstal of oplichting wanneer men met de verkregen codes geld bemachtigt, inbreuk op intellectueel-eigendomsrechten bij de inrichting van een nepsite, en wellicht aftappen van communicatie, als men de bestanddelen 'gegevens die niet voor hem zijn bestemd' en 'aftapt of opneemt' welwillend interpreteert (art. 139c Sr, iets waar opvallend veel van onze studenten mee op de proppen kwamen).
[4] HR 3 december 1996, *NJ* 1997, 574 m.nt.'tH.
[5] *Kamerstukken II 1989/90*, 21 551, nr. 3, p. 8: 'het gaat om gegevens die in het economisch verkeer verhandelbaar zijn'; de gegevens moeten 'reguliere handelswaar vertegenwoordigen'. Gebaseerd op Commissie Computercriminaliteit, *Informatietechniek & Strafrecht*, april 1987, p. 67-68.

handelsverkeer' komen te vervallen.[6] De wetgever sloot hier aan op het Europese kaderbesluit betaalmiddelenfraude[7]:

> 'hoewel het kaderbesluit op zichzelf niet vereist dat afpersing van een pincode strafbaar wordt gesteld, past [...] in het geheel van aanpassingen op het gebied van betaalpas- en betaalkaartfraude, waartoe het kaderbesluit wél verplicht, om ter bestrijding van fraude met en vervalsing van andere betaalmiddelen dan contanten, de strafbepaling betreffende afpersing zodanig te wijzigen, dat ook het onder bedreiging van geweld iemand te dwingen een pincode te noemen, strafbaar wordt.'[8]

In dit licht nu bevreemdt het dat de bepaling over oplichting niet op vergelijkbare wijze is aangepast. Fraude met betaalmiddelen is immers evenzeer – zo niet beter – mogelijk door slinkse listen en bedrog in te zetten als door geweld. De opkomst van phishing moet de maatschappij volgens ons minstens evenveel zorgen baren als pincodeafpersers. Het lijkt ons wenselijk dat de wetgever overweegt de oplichtingsbepaling in dezelfde zin als afpersing aan te passen, zodat ook het ontfutselen van pincodes, wachtwoorden en dergelijke strafbaar wordt.[9] Want hoewel er mogelijkheden zijn om op andere grondslagen een phisher te vervolgen, zal dat niet in alle gevallen soelaas bieden. Daarbij komt dat die andere vervolgingsmodaliteiten vaak betrekking hebben op het *gebruik* van de door phishing verkregen gegevens, bijvoorbeeld de onrechtmatige overboeking van geld. De hier voorgestelde aanpassing van art. 326 Sr brengt met name het verwerven van de voor een illegale transactie benodigde gegevens al onder het bereik van de strafwet. Daardoor kan onder omstandigheden niet alleen eerder worden ingegrepen, maar wordt tevens een *délit barrière* opgeworpen.[10] Dan wordt de phish eerder duur betaald door de dader dan door het slachtoffer.

Bert-Jaap Koops & Paul Wiemans
(*onderzoekers Universiteit van Tilburg*)

[6] *Stb*. 2004, 180, inwerkingtreding 16 juni 2004. Merk op dat dit een nogal ruime strafbaarstelling schept, want wie iemand onder dreiging van een pistool dwingt om zijn geboortedatum, favoriete acteur of de voetbaluitslagen van afgelopen zondag te noemen, is nu ook in theorie strafbaar, als hij tenminste beoogt daarmee enig voordeel te behalen.
[7] Besluit van de Raad van de Europese Unie van 28 mei 2001, betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten, *PbEG* 2001, L149.
[8] *Kamerstukken II* 2002/03, 29 025, nr. 3, p. 7.
[9] Gezien het veelal grensoverschrijdend karakter van phishing ligt het voor de hand om dit onderwerp ook bij de Europese Unie aan te kaarten, zodat het in een volgend kaderbesluit kan worden meegenomen.
[10] In deze constructie zal bijvoorbeeld het verzenden van een e-mail met een koppeling om in te loggen op een (nagemaakte) website van een bank, in combinatie met het exploiteren van die weblocatie, al een uitvoeringshandeling van oplichting, en daarmee een strafbare poging opleveren. Worden de gevraagde gegevens (rekeningnummer, toegangscode en dergelijke) daadwerkelijk ingevoerd, dan is het delict voltooid. Zonder de voorgestane aanpassing van art. 326 levert een en ander slechts een niet-strafbare voorbereidingshandeling op.